JOURNAL OF NUMBER THEORY 10, 510–522 (1978)

Iwasawa Invariants and Kummer Congruences

TAUNO METSÄNKYLÄ

Department of Mathematics, University of Turku, SF-20500 Turku, Finland

Communicated by H. W. Leopoldt

Received March 16, 1978

Let $f(x, \chi)$ be the Iwasawa power series for the p-adic L-function $L_p(s, \chi)$, where χ is an even nonprincipal character with conductor not divisible by p^2 (or by 8, when $p = 2$). The divisibility by p of the first p coefficients of $f(x, \chi)$ is characterized by Kummer type congruences of generalized Bernoulli numbers. Applications to Iwasawa invariants and class numbers of imaginary Abelian fields are discussed.

1. INTRODUCTION

Let p be a prime. Let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote the ring of p-adic integers and the field of p-adic numbers, respectively, and let Ω_p be an algebraic closure of $\mathbb{Q}_p$. In the following the field of all algebraic numbers is regarded as a subfield of Ω_p through a fixed embedding. Denote by ord the p-adic valuation on Ω_p, normalized so that $\operatorname{ord} p = 1$. Put $q = 4$ for $p = 2$ and $q = p$ for $p > 2$.

Consider a primitive character χ with conductor f_χ. Suppose that χ is nonprincipal, $\chi(-1) = 1$, and f_χ equals m or mq, where m is a natural number prime to p. Let $\mathfrak{o}_\chi$ be the ring of integers in the local subfield of Ω_p generated over $\mathbb{Q}_p$ by all the values of χ. According to Iwasawa's theory of p-adic L-functions [5], there exists a power series

$$f(x, \chi) = \sum_{k=0}^{\infty} a_k x^k \tag{1}$$

with $a_k = a_k(\chi) \in \mathfrak{o}_\chi$ such that

$$L_p(s, \chi) = 2f((1 + mq)^s - 1, \chi)$$

for all $s \in \mathbb{Z}_p$. This power series determines two remarkable invariants associated to χ, namely the numbers

$$\mu_\chi = \min\{\operatorname{ord} a_k(\chi) \mid k \geqslant 0\},$$
$$\lambda_\chi = \min\{k \mid k \geqslant 0, \operatorname{ord} a_k(\chi) = \mu_\chi\}.$$

0022-314X/78/0104–0510$02.00/0

The aim of this paper is to derive a relationship between ord $a_k(\chi)$, $k = 0, 1,\ldots, p-1$, and certain Kummer type congruences of generalized Bernoulli numbers (see Theorems 1 and 2). This gives us then information about μ_χ and λ_χ.

The numbers μ_χ and λ_χ are closely connected with the Iwasawa invariants μ and λ of imaginary Abelian fields. Let K be such a field, and write $\mu = \mu^+ + \mu^-$, $\lambda = \lambda^+ + \lambda^-$, where μ^+ and λ^+ are the corresponding invariants of the maximal real subfield of K. We may assume without loss of generality that the conductor of K is not divisible by qp (e.g., [22, p. 179]). Set

$$X = X(K) = \{\psi\omega \mid \psi \text{ an odd character of } K,\ \psi \neq \omega^{-1}\}, \tag{2}$$

where ω is the generating character mod q satisfying the congruence $\omega(a) \equiv a \pmod{q}$ for each unit a of $\mathbb{Z}_p$. Then

$$\mu^- = \sum_{\chi \in X} \mu_\chi, \qquad \lambda^- = \sum_{\chi \in X} \lambda_\chi$$

(see [3] or [11]).

For $n \geqslant 0$, let K_n denote the nth layer of the basic $\mathbb{Z}_p$-extension of K, and let h_n^- be its relative class number. The invariants μ^- and λ^- are related to ord h_n^-; for all sufficiently large n this relation can be expressed in the simple form

$$\text{ord } h_n^- = \mu^- p^n + \lambda^- n + c, \tag{3}$$

where c is a constant. Thus our considerations also give a connection between ord h_n^- and the generalized Bernoulli numbers. In particular, if K is the cyclotomic field of pth roots of unity ($p > 2$), then these generalized Bernoulli numbers reduce to ordinary Bernoulli numbers. In this case a number of known results about connections between ord h_n^- and the Bernoulli numbers [9, 13–15, 17–20] can be easily obtained from our results, as is seen in Section 4.

2. Two Lemmas on Generalized Bernoulli Numbers

Let $B^n(\chi)$ denote the nth generalized Bernoulli number belonging to the character χ. For the principal character ϵ, $B^n(\epsilon)$ is equal to the ordinary Bernoulli number B^n. As above, let m be a natural number prime to p, and write

$$C(m) = \{\chi \mid f_\chi = m \text{ or } f_\chi = mq,\ \chi(-1) = 1,\ \chi \neq \epsilon\},$$
$$C_1(m) = \{\chi \mid f_\chi = m\}.$$

LEMMA 1. *Let $p > 2$ and $\chi_1 \in C_1(m)$. Then*

$$B^n(\chi_1\omega^t) \equiv B^{tp^{2k}+n}(\chi_1) \pmod{p^k}$$

for $n \geqslant 1$, $k \geqslant 0$, and $0 \leqslant t \leqslant p-2$.

Proof. Put $\chi = \chi_1\omega^t$. Since f_χ divides mp^{k+1}, we have (in the usual symbolic notation)

$$\sum_{a=1}^{mp^{k+1}} \chi(a)\, a^n = \frac{1}{n+1}\left[(B(\chi) + mp^{k+1})^{n+1} - B^{n+1}(\chi)\right]$$

$$= mp^{k+1}B^n(\chi) + \sum_{i=2}^{n+1} \frac{1}{n+1}\binom{n+1}{i} B^{n+1-i}(\chi)\, m^i p^{(k+1)i}.$$

Writing the terms of the last sum in the form

$$\frac{p^{i-2}}{i}\binom{n}{i-1} pB^{n+1-i}(\chi)\, m^i p^{ki+1},$$

we find that

$$\sum_{a=1}^{mp^{k+1}} \chi(a)\, a^n \equiv mp^{k+1}B^n(\chi) \pmod{p^{2k+1}}.$$

In view of

$$\chi(a) = \chi_1(a)\,\omega^t(a) \equiv \chi_1(a)\, a^{tp^{2k}} \pmod{p^{2k+1}},$$

this proves the lemma.

The last congruence is not true for, say, $t = p-1$, when a is chosen appropriately (as $\omega^{p-1} = \epsilon$). Note also that the absence of a suitable analog of this congruence for $p = 2$ compels us to restrict Lemma 1 to odd primes p.

Let us drop this restriction and put

$$\alpha_n = (1 + mq)^{-n} - 1 \qquad (n = 0, 1, \ldots).$$

For $\chi \in C(m)$, let $f(x, \chi) = a_0 + a_1x + a_2x^2 + \cdots$ be the power series introduced in Section 1. Then

$$2f(\alpha_n, \chi) = L_p(-n, \chi) = -(1 - (\chi\omega^{-n-1})(p)\, p^n)\frac{B^{n+1}(\chi\omega^{-n-1})}{n+1}. \quad (4)$$

For any sequence $x_0, x_1, \ldots$ in Ω_p, define the difference operator Δ_c ($c \geqslant 1$), as usual, by $\Delta_c x_n = x_{n+c} - x_n$. Set $\Delta_1 = \Delta$. Below we need the following elementary property of these operators: If $c \mid d$, then $\Delta_d = g(\Delta_c)\Delta_c$, where $g(x)$ is a polynomial in $\mathbb{Z}[x]$.

LEMMA 2. *Let $\chi \in C(m)$. For $h \geqslant 0$ and $n \geqslant 0$,*

$$\Delta^h f(\alpha_n, \chi) \equiv (-mq)^h \sum_{k=0}^{h} k!\, a_k S_2(h, k) \pmod{q^{h+1}},$$

where $S_2(h, k)$ denotes the Stirling number of the second kind.

Proof. We have

$$\Delta^h f(\alpha_n, \chi) = \Delta^h \sum_{k=0}^{\infty} a_k \alpha_n{}^k \equiv \sum_{k=0}^{h} a_k \Delta^h \alpha_n{}^k \pmod{q^{h+1}},$$

because $\alpha_n \equiv 0 \pmod{q}$.

For $h = 0$ our assertion reads as $f(\alpha_n, \chi) \equiv a_0 \pmod{q}$; this is trivially true. Let $h \geqslant 1$. Then

$$\Delta^h \alpha_n{}^k = \Delta^h((1 + mq)^{-n} - 1)^k = \sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} \Delta^h (1 + mq)^{-nu},$$

where, furthermore,

$$\Delta^h (1 + mq)^{-nu} = (1 + mq)^{-nu}((1 + mq)^{-u} - 1)^h \equiv (-mqu)^h \pmod{q^{h+1}}.$$

Observing that

$$\sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} u^h = \Delta^k 0^h = k!\, S_2(h, k)$$

[16, p. 202], we get from this the congruence of the lemma.

Now let $\chi_1 \in C_1(m)$. A by-product from Lemma 2 is that

$$\sum_{u=0}^{h} (-1)^{h-u} \binom{h}{u} f(\alpha_{n+u}, \chi_1 \omega^{n+1}) \equiv 0 \pmod{q^h} \quad (h = 0, 1, \ldots),$$

when n is so chosen ($n \geqslant 0$) that $\chi_1 \omega^{n+1}$ is even and nonprincipal. This allows us to conclude, by (4), that

$$\Delta^h_{\phi(q)}(1 - \chi_1(p)\, p^n) \frac{B^{n+1}(\chi_1)}{n+1} \equiv 0 \pmod{q^{h+1} p^{-1}} \tag{5}$$

provided $\chi_1 \omega^{n+1} \neq \epsilon$ (note that $B^{n+1}(\chi_1) = 0$ when $\chi_1 \omega^{n+1}$ is odd). Here ϕ denotes Euler's ϕ-function. By considering the last congruence for $h = 0$ we find that

$$\frac{1}{n+1} B^{n+1}(\chi_1) \equiv 0 \pmod{qp^{-1}}, \tag{6}$$

whenever $n \geqslant 1$ and $\chi_1\omega^{n+1} \neq \epsilon$. Combined with (5) this gives us the Kummer congruences

$$\Delta^h_{\phi(q)} \frac{1}{n+1} B^{n+1}(\chi_1) \equiv 0 \pmod{q^{h+1}p^{-1}} \quad (h = 1, 2,\ldots) \tag{7}$$

valid for $n \geqslant h$ when $p > 2$ and for $n \geqslant 2h$ when $p = 2$, under the additional restriction $\chi_1\omega^{n+1} \neq \epsilon$. This restriction excludes merely the case $\chi_1 = \epsilon$, $n + 1 \equiv 0 \pmod{p-1}$. We need (5), (6), and (7) in the sequel.

It should be noted that (6) and (7), for $p > 2$, were proved by Carlitz [1] and are in fact valid for a larger class of characters (cf. also [12]).

3. The Divisibility by p of the First Coefficients a_k

Let us consider the power series (1) for a character $\chi \in C(m)$. Suppose that $r \in \mathbb{Q}$, $0 < r \leqslant 1$.

Theorem 1. *Let $\chi \in C(m)$ and let n be a nonnegative integer. The following conditions* (I) *and* (II) *are equivalent, provided* $0 \leqslant h \leqslant p - 1$:

(I) $a_k(\chi) \equiv 0 \pmod{p^r}$ *for* $k = 0, 1,\ldots, h$;

(II) $\Delta^k f(\alpha_n, \chi) \equiv 0 \pmod{q^k p^r}$ *for* $k = 0, 1,\ldots, h$.

Proof. It is a direct consequence of Lemma 2 that (I) implies (II). We verify the converse implication by induction on h.

Since $f(\alpha_n, \chi) \equiv a_0 \pmod{q}$, the assertion is true for $h = 0$. Suppose that it is true for all values of h less than a fixed $h \geqslant 1$. Now, if (II) holds for this h, then $\Delta^h f(\alpha_n, \chi) \equiv 0 \pmod{q^h p^r}$ and so, by Lemma 2,

$$\sum_{k=0}^{h-1} k!\, a_k S_2(h, k) + h!\, a_h \equiv 0 \pmod{p^r}.$$

By induction hypothesis, $a_k \equiv 0 \pmod{p^r}$ for $k = 0, 1,\ldots, h-1$. But $\operatorname{ord}(h!) = 1$, and therefore $a_h \equiv 0 \pmod{p^r}$ as was to be proved.

Remark. Suppose that the congruences (II) (and hence also (I)) are valid for $k = 0, 1,\ldots, p-1$. Since $k! \equiv 0 \pmod{p}$ for all $k \geqslant p$, it then follows from Lemma 2 that $\Delta^h f(\alpha_n, \chi) \equiv 0 \pmod{q^h p^r}$, whenever $h \geqslant p$. Consequently, Theorem 1 cannot be true without the restriction $h \leqslant p - 1$.

Theorem 2. *Let $\chi \in C(m)$ and put $\chi = \chi_1\omega^t$ with $\chi_1 \in C_1(m)$ and $0 \leqslant t \leqslant \phi(q) - 1$. Suppose that $0 \leqslant h \leqslant p - 1$. If*

$$\Delta^k f(\alpha_n, \chi) \equiv 0 \pmod{q^k p^r}, \quad k = 0, 1,\ldots, h, \tag{8}$$

for some $n \geqslant 0$, then

$$\Delta^k_{\phi(q)}(1 - \chi_1(p)\, p^{n-1}) \frac{B^n(\chi_1)}{n} \equiv 0 \pmod{q^{k+1}p^{r-1}}, \quad k = 0, 1, \ldots, h, \quad (9)$$

whenever $n \geqslant 1$ and $n \equiv t \pmod{p-1}$. Conversely, if $p > 2$ and (9) is valid for some n subject to the conditions $n \geqslant 1$, $n \equiv t \pmod{p-1}$, then (8) holds for all $n \geqslant 0$.

Proof. First note that, by Theorem 1, the validity of the congruences (8) for some $n \geqslant 0$ implies their validity for all $n \geqslant 0$.

Suppose that (8) holds, and choose n so that $n \geqslant 1$ and $n \equiv t \pmod{p-1}$. Then $\Delta^k f(\alpha_{n-1}, \chi_1\omega^t) \equiv 0 \pmod{q^k p^r}$ for $k = 0, 1, \ldots, h$. Since $\omega^{t-n} = \epsilon$, the same argument as before (see (5)) gives us (9).

To prove the converse part, let $p > 2$, fix k such that $0 \leqslant k \leqslant h$, and suppose that

$$\Delta^k_{p-1}(1 - \chi_1(p)\, p^{n-1}) \frac{B^n(\chi_1)}{n} \equiv 0 \pmod{p^{k+r}} \quad (10)$$

for some n satisfying the conditions $n \geqslant 1$, $n \equiv t \pmod{p-1}$. By virtue of $\chi_1\omega^n = \chi \neq \epsilon$ it follows from (5) that (10) also holds with Δ^k_{p-1} replaced by Δ^{k+1}_{p-1}. Using the identity $\Delta^k_{p-1}x_n + \Delta^{k+1}_{p-1}x_n = \Delta^k_{p-1}x_{n+p-1}$ we therefore see that (10) is valid for every n greater than our original n and congruent to $t \pmod{p-1}$. Let us fix such an n so that $n \geqslant 2p$.

In (10) one can replace Δ^k_{p-1} by Δ^k_d, where $d = p^s - 1$ with $s \geqslant 1$. Thus (10) yields the congruence

$$\sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} \frac{B^{n+u(p^s-1)}(\chi_1)}{n-u} \equiv 0 \pmod{p^{k+r}} \quad (11)$$

valid for all sufficiently large s. Furthermore, for the quotient appearing here on the left-hand side we have

$$\frac{B^{n+u(p^s-1)}(\chi_1)}{n-u} \equiv \frac{B^{n-u}(\chi_1\omega^u)}{n-u} \pmod{p^{k+r}}, \quad (12)$$

whenever s is large enough. This follows from Lemma 1 in case $0 \leqslant u \leqslant p-2$, and from Kummer's congruences in case $u = p-1$ (see (7) and note that n was chosen large enough).

On inserting (12) in (11) and changing the summation variable from u to $k-u$ we obtain

$$\sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} \frac{B^{n-k+u}(\chi_1\omega^{k-u})}{n-k+u} \equiv 0 \pmod{p^{k+r}}.$$

This congruence remains valid when each term of the sum is multiplied by $1 - (\chi_1\omega^{k-u})(p)\,p^{n-k+u-1}$. Hence we infer that

$$\Delta^k f(\alpha_{n-k-1}, \chi_1\omega^t) \equiv 0 \pmod{p^{k+r}},$$

and the proof is completed.

THEOREM 3. *Theorem 2 remains true if* (9) *is replaced by*

$$\Delta^k_{\phi(q)} \frac{1}{n} B^n(\chi_1) \equiv 0 \pmod{q^{k+1}p^{r-1}}, \qquad k = 0, 1, \ldots, h, \tag{13}$$

and instead of the condition $n \geqslant 1$ *it is assumed that* $n \geqslant \max(2, h+1)$ *when* $p > 2$ *and* $n \geqslant \max(2, 2h+1)$ *when* $p = 2$.

Proof. Let n satisfy the stronger conditions mentioned in the theorem, and suppose that $n \equiv t \pmod{p-1}$. We have only to show that both (9) and (13) imply the congruences

$$\Delta^k_{\phi(q)} p^{n-1} B^n(\chi_1)/n \equiv 0 \pmod{q^{k+1}p^{r-1}}, \quad k = 0, 1, \ldots, h.$$

Here the left-hand side is congruent to $p^{n-1}B^n(\chi_1)/n \pmod{q^{k+1}p^{r-1}}$, for n was supposed so large that, by (6),

$$p^{n-1+u\phi(q)} \frac{B^{n+u\phi(q)}(\chi_1)}{n + u\phi(q)} \equiv 0 \pmod{q^{h+1}p^{r-1}},$$

whenever $u \geqslant 1$. On the other hand, it follows from both (9) and (13), for $h = 0$, that $B^n(\chi_1)/n \equiv 0 \pmod{qp^{r-1}}$. Hence $p^{n-1}B^n(\chi_1)/n \equiv 0 \pmod{q^{k+1}p^{r-1}}$, and the assertion is proved.

By combining the above three theorems we obtain information about μ_χ and λ_χ, for $\chi = \chi_1\omega^t \in C(m)$, in terms of the numbers $B^n(\chi_1)$. For example, if $\mu_\chi > 0$ then the congruences (9) hold for $k = 0, 1, \ldots, p-1$, a result which was also proved, essentially, by Shiratani [17, p. 134] in the specific case $\chi_1 = \epsilon$. This case is treated in detail in the following section.

4. APPLICATION TO CYCLOTOMIC FIELDS WITH PRIME POWER CONDUCTOR

Let $p > 2$ and let K be the cyclotomic field of pth roots of unity. Then $X(K)$, the associated set of characters defined by (2), consists of the characters ω^t, where t runs through the set $N_p = \{2, 4, \ldots, p-3\}$. (Note that $X(K)$ is empty for $p = 3$.) Moreover, the nth layer of the basic $\mathbb{Z}_p$-extension of K is the cyclotomic field of p^{n+1}th roots of unity ($n \geqslant 0$). Let h_n^- be its relative class number.

THEOREM 4. *Let $t \in N_p$ and $0 \leqslant h \leqslant p-1$. Then*

$$a_k(\omega^t) \equiv 0 \pmod{p}, \quad k = 0, 1, \ldots, h,$$

if and only if

$$\Delta_{p-1}^k (1 - p^{t-1}) \frac{B^t}{t} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, h,$$

or equivalently,

$$\Delta_{p-1}^k \frac{B^n}{n} = \sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} \frac{B^{n+u(p-1)}}{n + u(p-1)} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, h,$$

where n satisfies the conditions $n \geqslant h+1$ and $n \equiv t \pmod{p-1}$.

Proof. Since $\omega^t \in C(1)$, we get the theorem immediately on applying Theorem 1 in conjunction with Theorems 2 and 3.

It should be noted that the cases $h = 0$ and $h = 1$ of Theorem 4 appear already in [10, pp. 67–68]. For $h = 0$ this theorem states that $a_0(\omega^t) \equiv 0 \pmod{p}$ if and only if $B^t \equiv 0 \pmod{p}$, i.e., (p, t) is an irregular pair. Because

$$\operatorname{ord} h_0^- = \sum_{t \in N_p} \operatorname{ord} f(0, \omega^t) = \sum_{t \in N_p} \operatorname{ord} a_0(\omega^t) \tag{14}$$

(see [6, pp. 91, 95]), this gives us the following well-known results: $\operatorname{ord} h_0^- > 0$ if and only if $B^t \equiv 0 \pmod{p}$ for some $t \in N_p$; and $\operatorname{ord} h_0^- \geqslant i_p$, where i_p is the number of such $t \in N_p$ (the index of irregularity of p). The former result is a classical theorem of Kummer [9], the latter follows from Vandiver's theorem [19].

A link between the power series $f(x, \omega^t)$ and the values of $\operatorname{ord} h_n^-$, $n \geqslant 0$, is provided by the following relation, due to Iwasawa [6, p. 92]:

$$\operatorname{ord}(h_{n+1}^-/h_n^-) = \sum_{t \in N_p} D_n{}^t \qquad (n = 0, 1, \ldots) \tag{15}$$

with

$$D_n{}^t = \sum_{\zeta \in W_{n+1}} \operatorname{ord} f(\zeta - 1, \omega^t),$$

where W_n stands for the set of primitive p^n-th roots of unity. Since $\operatorname{ord}(\zeta - 1)$ is independent of the choice of $\zeta \in W_{n+1}$, we may also write

$$D_n{}^t = \phi(p^{n+1}) \operatorname{ord} f(\zeta - 1, \omega^t) \qquad (\zeta \in W_{n+1}).$$

We briefly discuss some implications of (15) in the light of Theorem 4.

PROPOSITION 1. *Let $n \geqslant 0$ and $0 \leqslant j \leqslant \phi(p^{n+1}) - 1$. Then*

$$a_0(\omega^t) \equiv a_1(\omega^t) \equiv \cdots \equiv a_{j-1}(\omega^t) \equiv 0, \qquad a_j(\omega^t) \not\equiv 0 \pmod{p}, \quad (16)$$

implies that $D_n{}^t = j$, and vice versa.

Proof. It follows easily from (16) that

$$\operatorname{ord} f(\zeta - 1, \omega^t) = \operatorname{ord} a_j(\zeta - 1)^j = j/\phi(p^{n+1}),$$

that is, $D_n{}^t = j$. Conversely, let $\operatorname{ord} f(\zeta - 1, \omega^t) = j/\phi(p^{n+1})$. If $a_k \equiv 0 \pmod{p}$ for $k = 0, 1, \ldots, \phi(p^{n+1}) - 1$, then

$$\operatorname{ord} f(\zeta - 1, \omega^t) \geqslant \min_{k \geqslant 0} \operatorname{ord} a_k(\zeta - 1)^k \geqslant 1,$$

which is a contradiction. Hence there exists a k such that $a_k \not\equiv 0 \pmod{p}$ and $0 \leqslant k \leqslant \phi(p^{n+1}) - 1$. If k is the least index satisfying these conditions, then $\operatorname{ord} f(\zeta - 1, \omega^t) = k/\phi(p^{n+1})$ and so $j = k$. Therefore (16) holds true.

Combining this proposition with Theorem 4, for $j = 0$ and $j = 1$, we obtain the following known results about $\sigma_n = \operatorname{ord}(h_{n-1}^-/h_n^-)$, where $n \geqslant 0$:

(i) $\sigma_n > 0$ if and only if $B^t \equiv 0 \pmod{p}$ for some $t \in N_p$ (e.g., [20]);

(ii) $\sigma_n \geqslant i_p$, and $\sigma_n > i_p$ if and only if

$$B^t \equiv 0 \pmod{p}, \qquad \frac{B^t}{t} \equiv \frac{B^{t+p-1}}{t+p-1} \pmod{p^2} \qquad (17)$$

for some $t \in N_p$ [15, 13];

(iii) $\sigma_n \geqslant i_p + j_p$, where j_p is the number of such $t \in N_p$ for which (17) holds [14].

Similar arguments extended to larger values of j show that:

(iv) A necessary and sufficient condition for $D_n{}^t = j$, with $n \geqslant 0$ and $0 \leqslant j \leqslant p - 2$, is that the congruence

$$\sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} (1 - p^{t-1+u(p-1)}) \frac{B^{t+u(p-1)}}{t + u(p-1)} \equiv 0 \pmod{p^{k+1}} \quad (18)$$

be valid for $k = 0, 1, \ldots, j - 1$ but not for $k = j$;

(v) A necessary and sufficient condition for $D_n{}^t \geqslant j$, with $n \geqslant 0$ and $0 \leqslant j \leqslant p - 1$ (or also $n \geqslant 1$ and $j = p$), is that (18) be valid for $k = 0, 1, \ldots, j - 1$.

The last result has been proved by Shiratani [18] in a slightly weaker form (for larger values of n).

Note that (16) is nothing but an equivalent form for the statement $\mu_\chi = 0$,

$\lambda_\chi = j$, where $\chi = \omega^t$. Writing $f(x, \chi) = p^{\mu_\chi} \sum_{k \geqslant 0} a_k' x^k$ and considering a_k' instead of a_k we arrive at the following statement analogous to the first part of Proposition 1: If $n \geqslant 0$ and, for $\chi = \omega^t$, $0 \leqslant \lambda_\chi \leqslant \phi(p^{n+1}) - 1$, then $D_n{}^t = \mu_\chi \phi(p^{n+1}) + \lambda_\chi$. Accordingly,

$$\operatorname{ord}(h_{n+1}^-/h_n^-) = \mu^- \phi(p^{n+1}) + \lambda^-,$$

when n is so large that $\phi(p^{n+1}) > \lambda_\chi$ for all $\chi = \omega^t \in X(K)$. This implies the fundamental formula (3) in the special case under consideration. (In fact, it is essentially this reasoning that leads to (3) in [6, pp. 92–94], where only the lower bound for n is weaker.) Particularly, assuming that $\lambda_\chi < p - 1$ for all $\chi \in X(K)$ we infer that

$$\operatorname{ord} h_n^- = \mu^- p^n + \lambda^- n + (\operatorname{ord} h_0^- - \mu^-)$$

for all $n \geqslant 0$. Moreover, it is seen from (14) that the "constant term" $\operatorname{ord} h_0^- - \mu^-$ here is nonnegative.

The validity of the congruences (17) has been tested numerically for all $t \in N_p$ up to $p < 125{,}000$ (see [8, 21]). In all these cases (17) fails and hence $\mu_\chi = 0$ and $\lambda_\chi = 0$ or 1 for $\chi = \omega^t$. (This result has been obtained by other methods, too.) Furthermore, $\operatorname{ord} h_0^- = i_p$ and so

$$\operatorname{ord} h_n^- = i_p n + i_p \qquad (n \geqslant 0)$$

for $p < 125{,}000$ (cf. [7, p. 92]). Note also that for all these p we have $\operatorname{ord} h_n^- = \operatorname{ord} h_n$, where h_n is the class number of K_n.

5. Further Applications

Consider first the character set associated to the cyclotomic field K of $4p$th roots of unity, where $p > 2$. In addition to the characters $\omega^t \in C(1)$ discussed above this set contains the characters $\chi \in C(4)$, i.e., the characters of the form $\theta\omega^t$, where t is odd and θ indicates the unique character with $f_\theta = 4$. Observe that $2B^n(\theta) = -nE^{n-1}$ $(n \geqslant 1)$, where E^n denotes the nth Euler number. Thus one can formulate the following analog of Theorem 4.

Theorem 5. *Let $\chi = \theta\omega^t$, where t is odd, $1 \leqslant t \leqslant p - 2$, and suppose that $0 \leqslant h \leqslant p - 1$. Then*

$$a_k(\chi) \equiv 0 \pmod{p}, \qquad k = 0, 1, \ldots, h,$$

if and only if

$$\Delta_{p-1}^k (1 - \theta(p)\, p^{t-1})\, E^{t-1} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, h,$$

or equivalently,

$$\Delta_{p-1}^{k} E^{n} = \sum_{u=0}^{k} (-1)^{k-u} \binom{k}{u} E^{n+u(p-1)} \equiv 0 \pmod{p^{k+1}}, \quad k = 0, 1, \ldots, h,$$

where n satisfies the conditions $n \geqslant \max(1, h)$ *and* $n \equiv t - 1 \pmod{p-1}$.

It follows in particular that $a_0(\chi) \equiv 0 \pmod{p}$ if and only if

$$1 - \theta(p) \equiv 0 \pmod{p}, \quad \text{when} \quad \chi = \theta\omega,$$
$$E^{t-1} \equiv 0 \pmod{p}, \quad \text{when} \quad \chi = \theta\omega^{t} \in X(K), \quad 3 \leqslant t \leqslant p-2.$$

The former congruence is equivalent to $p \equiv 1 \pmod 4$, while the latter is true if and only if $(p, t-1)$ is an E-irregular pair. This result as well as some more general implications of Theorem 5 of course have consequences concerning $\operatorname{ord} h_n^-$, similar to those presented in the preceding section (h_n^- the relative class number of the $4p^{n+1}$th cyclotomic field).

The special cases $h = 0$ and $h = 1$ of Theorem 5 were proved also in [2], where the invariants μ_χ and λ_χ were determined for all $\chi = \theta\omega^t \in X(K)$ up to $p < 10^4$. Like the characters of Section 4, all the present characters proved to be trivial in the sense that always $\mu_\chi = 0$ and $\lambda_\chi = 0$ or 1.

For $p \equiv 1 \pmod 4$, the congruence $a_0(\theta\omega) \equiv 0 \pmod{p}$ verified above can actually be sharpened to the form $a_0(\theta\omega) = 0$. This is seen from the following more general result.

PROPOSITION 2. *Let* $p > 2$ *and let* $\chi = \chi_1\omega \in C(m)$ *with* $\chi_1 \in C_1(m)$. *If* $\chi_1(p) = 1$, *then* $a_0(\chi) = 0$ *and hence either* μ_χ *or* λ_χ *is positive.*

Proof. Use (4) and the fact that $\alpha_0 = 0$, to write

$$2a_0 = 2f(\alpha_0, \chi) = -(1 - \chi_1(p))\, B^1(\chi_1) = 0.$$

In conclusion we shall deal with an example of a nontrivial $f(x, \chi)$. Let $p = 3$ and let ψ be the odd real character with $f_\psi = m = 56$, i.e., the character of the quadratic field $\mathbb{Q}((-14)^{1/2})$. It is known that, for $p = 3$, this field has $\mu = 0$ and $\lambda \geqslant 2$ [4, p. 373]. Obviously $\mu = \mu_{\psi\omega}$ and $\lambda = \lambda_{\psi\omega}$ in this case.

Since $\psi(3) = 1$, Proposition 2 tells us that either $\mu > 0$ or $\lambda > 0$. Moreover, a simple but somewhat tedious calculation shows that

$$B^3(\psi) \equiv -3^3 \pmod{3^4}, \qquad B^5(\psi) \equiv 0 \pmod{3^3}$$

(apply, e.g., the formula $mB^n(\psi) = -\sum_{a=1}^{m} \psi(a)(mB - a)^n$). For brevity, put $A_n = (1 - 3^{n-1})\, B^n(\psi)/n$. It follows that

$$A_1 - A_3 \equiv 0 \pmod{3^2},$$
$$A_1 - 2A_3 + A_5 \equiv -3^2 \not\equiv 0 \pmod{3^3}.$$

Thus we obtain the result that $\mu = 0$ and $\lambda = 2$.

REFERENCES

1. L. CARLITZ, Arithmetic properties of generalized Bernoulli numbers, *J. Reine Angew. Math.* **202** (1959), 174–182.
2. R. ERNVALL AND T. METSÄNKYLÄ, Cyclotomic invariants and E-irregular primes, *Math. Comp.*, to appear.
3. B. E. FERRERO, "Iwasawa Invariants of Abelian Number Fields," Ph.D. Thesis, Princeton University, 1975.
4. R. GOLD, The nontriviality of certain Z_l-extensions, *J. Number Theory* **6** (1974), 369–373.
5. K. IWASAWA, On p-adic L-functions, *Ann. of Math.* **89** (1969), 198–205.
6. K. IWASAWA, "Lectures on p-adic L-functions," Annals of Mathematics Studies, No. 74, Princeton Univ. Press, Princeton, N.J., 1972.
7. K. IWASAWA AND C. SIMS, Computation of invariants in the theory of cyclotomic fields, *J. Math. Soc. Japan* **18** (1966), 86–96.
8. W. JOHNSON, Irregular prime divisors of the Bernoulli numbers, *Math. Comp.* **28** (1974), 653–657.
9. E. E. KUMMER, Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λ-ten Wurzeln der Einheit gebildeten complexen Zahlen, *J. Reine Angew. Math.* **40** (1850), 117–129; "Collected papers," Vol. I, pp. 323–335, Springer-Verlag, Berlin, 1975.
10. T. METSÄNKYLÄ, On the cyclotomic invariants of Iwasawa, *Math. Scand.* **37** (1975), 61–75.
11. T. METSÄNKYLÄ, On the Iwasawa invariants of imaginary abelian fields, *Ann. Acad. Sci. Fenn. Ser. A I* **1** (1975), 343–353.
12. T. METSÄNKYLÄ, Note on certain congruences for generalized Bernoulli numbers, *Arch. Math. (Basel)*, to appear.
13. T. MORISHIMA, Über die Einheiten und Idealklassen des Galoisschen Zahlkörpers und die Theorie der Kreiskörper der l^ν-ten Einheitswurzeln, *Japan. J. Math.* **10** (1933), 83–126.
14. T. MORISHIMA, Über die Theorie der Kreiskörper der l^ν-ten Einheitswurzeln II, *Japan. J. Math.* **11** (1934), 225–240.
15. F. POLLACZEK, Über die irregulären Kreiskörper der l-ten und l^2-ten Einheitswurzeln, *Math. Z.* **21** (1924), 1–38.
16. J. RIORDAN, "Combinatorial Identities," Wiley, New York, 1968.
17. K. SHIRATANI, On some relations between Bernoulli numbers and class numbers of cyclotomic fields, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **18** (1964), 127–135.
18. K. SHIRATANI, Ein Satz zu den Relativklassenzahlen der Kreiskörper, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **21** (1967), 132–137.
19. H. S. VANDIVER, On the first factor of the class number of a cyclotomic field, *Bull. Amer. Math. Soc.* **25** (1919), 458–461.

20. H. S. VANDIVER, On the class number of the field $\Omega(e^{2i\pi/p^n})$ and the second case of Fermat's last theorem, *Proc. Nat. Acad. Sci.* **6** (1920), 416–421.
21. S. S. WAGSTAFF, JR., The irregular primes to 125000, *Math. Comp.*, to appear.
22. L. C. WASHINGTON, Class numbers and Z_p-extensions, *Math. Ann.* **214** (1975), 177–193.